Module 5 | Exploitation

Introduction

All the recon, spoofing, and password cracking you've been doing has lead you here - exploitation! At this point, you should know how you're going to attack a system, and you should be building the tools you need (or finding the tools you need) to exploit vulnerabilities in some way.

Exploitation is pretty important to both offensive and defensive cybersecurity. This is another point at which defenders can stop an attack; for attackers, it's not a step they can miss.

Learning Objectives

We'll continue to focus on learning cybersecurity concepts and techniques so you'll be able to *(1) design and execute, and (2) defend against a malware campaign against a target* (Objective E). We also want to be able to *trace execution of a program via generated disassembly* (Objective E.e) by the time we complete this module.

Notes: This module has an end of module assignment.

All homework needs to be submitted from this module by the end of the fifth week. The assignment will make use of GDB and Ubuntu LTS. Get Ubuntu from the Ubuntu site (http://www.ubuntu.com). You'll install GDB in your Ubuntu distribution during the lectures. By the end of this module, you'll be able to use a binary debugger to analyze a program I've written and find hidden information.

Required Instructional Materials

As usual, all you'll need for this section are the video lectures and the tooling and techniques we cover. You may want to refer to specific noted websites or sites associated with the tools we discuss as you go through your assignment. You'll need an internet connection to access, install, and read about the tools we discuss.

Summary

This module consists of videos and a module assignment. This module is dedicated to various exploitation techniques.

If you have questions about some aspect of Learn, **UNM LEARN Support** is available to troubleshoot technical problems.

Contact them 24/7 at 505-277-0857, 1-877-688-8817 or use the "Create a Support Ticket" link on the left Course Menu.